FORTINET
High Performance Network Security

FortiOS™ Handbook - Hardening your FortiGate

VERSION 5.4.0

FORTIOS
5.4
VERSION

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

CLI REFERENCE

http://cli.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

3/15/2017

FortiOS™ Handbook - Hardening your FortiGate

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-03-15	Official release.

Introduction

This document describes a series of techniques used to improve the security of administrative access to a FortiGate device.

The following sections are included:

Install the FortiGate unit in a physically secure location

A good place to start with is physical security. Install the FortiGate unit in a secure location, such as a locked room or a room with restricted access. This way unauthorized users can't get physical access to the device.

If unauthorized users have physical access they can disrupt your entire network by disconnecting your FortiGate unit (either by accident or on purpose). They could also connect a console cable and attempt to log into the CLI. Also, when a FortiGate unit reboots, a person with physical access can interrupt the boot process and install different firmware.

Maintain the firmware

On installation of a new firewall, it is necessary to update the firmware to the latest version provided by the manufacturer.

Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues. After you have registered your FortiGate unit, you can download firmware updates from the support web site, https://support.fortinet.com.

Before you install any new firmware, be sure to follow the steps below:

- Review the Release Notes for a new firmware release.
- Review the Supported Upgrade Paths document to make sure the upgrade from your current image to the desired new image is supported.
- Backup the current configuration, including local certificates.
- Test the new firmware until you are satisfied that it applies to your configuration.

Installing new firmware without reviewing release notes or testing the firmware may result in changes to settings or unexpected issues.

Only FortiGate admin users and administrators whose access profiles contain system read and write privileges can change the FortiGate firmware.

Add new administrator accounts

Rather than allowing all administrators to access the FortiGate unit with the admin administrator account you should create administrator accounts for each person that requires administrative access. That way you can track who has made configuration changes and performed other administrative activities. Keep the number of administrative accounts to a minimum to keep better control on who can access the device.

To add administrators go to **System > Admin Profiles** and select **Create New**.

If you want administrators to have access to all FortiGate configuration options, their accounts should have the **prof_admin** admin profile. Administrators with this profile can do anything except add new administrator accounts.

At least one account should always have the **super_admin** profile as this profile is required to add and remove administrators. To improve security only a very few administrators (usually one) should be able to add new administrators.

If you want some administrator accounts to have limited access to the FortiGate configuration you can create custom admin profiles that only allow access to selected parts of the configuration. To add custom admin profiles, go to **System > Admin Profiles** and select **Create New**.

For example, if you want to add an admin profile that does not allow changing firewall policies, when you configure the admin profile set **Firewall Configuration** to **None** or **Read Only**.

Change the admin account name and limit access to this account

The default super_admin administrator account, admin, is a well known administrator name so if this account is available it could be easier for attackers to access the FortiGate unit because they know they can log in with this name, only having to determine the password. You can improve security by changing this name to one more difficult for an attacker to guess.

To do this, create a new administrator account with the super_admin admin profile and log in as that administrator. Then go to **System > Administrators** and edit the admin administrator and change the Administrator name.

Once the account has been renamed you could delete the super_admin account that you just added. Consider also only using the super-admin account for adding or changing administrators. The less this account is used to

less likely that it could be compromised. You could also store the account name and password for this account in a secure location in case for some reason the account name or password is forgotten.

Only allow administrative access to the external interface when needed

When possible, don't allow administration access on the external interface and use internal access methods such as IPsec VPN or SSL VPN.

To disable administrative access on the external interface, go to **Network > Interfaces,** edit the external interface and disable HTTPS, PING, HTTP, SSH, and TELNET under **Administrative Access.**

This can also be done with CLI using following commands:

```
config system interface
   edit <external_interface_name>
   unset allowaccess
end
```

Please note that this will disable all services on the external interface including CAPWAP, FMG-Access, and SNMP. If you need some of these services enabled on your external interface, for example CAPWAP and FMG-Access to ensure connectivity between FortiGate unit and respectively FortiAP and FortiManager, then you need to use following CLI command:

```
config system interface
   edit <external_interface_name>
   set allowaccess capwap fgfm
end
```

When enabling remote access, configure Trusted Hosts and Two-factor Authentication

If you have to have remote access and can't use IPsec or SSL VPN then you should only allow HTTPS and SSH and use secure access methods such as trusted hosts and Two-factor authentication.

Configuring Trusted Hosts

Setting trusted hosts for administrators limits what computers an administrator can log in the FortiGate unit from. When you identify a trusted host, the FortiGate unit will only accept the administrator's login from the configured IP address or subnet. Any attempt to log in with the same credentials from any other IP address or any other subnet will be dropped. To ensure the administrator has access from different locations, you can enter up to ten IP addresses or subnets. Ideally, this should be kept to a minimum. For higher security, use an IP address with a net mask of 255.255.255.255, and enter an IP address (non-zero) in each of the three default trusted host fields.

Trusted hosts are configured when adding a new administrator by going to System > Administrators in the web-based manager and selecting **Restrict this Admin Login from Trusted Hosts Only**, or `config system admin` in the CLI.

The trusted hosts apply to the web-based manager, ping, snmp and the CLI when accessed through SSH. CLI access through the console port is not affected.

Also ensure all entries contain actual IP addresses, not the default 0.0.0.0.

Configuring Two-factor Authentication

FortiOS 5.0 provides support for FortiToken and FortiToken Mobile. FortiToken Mobile is a Fortinet application that enables you to generate One Time Passwords (OTPs) on a mobile device for FortiGate two-factor authentication. The user's mobile device and the FortiGate unit must be connected to the Internet to activate FortiToken mobile. Once activated, users can generate OTPs on their mobile device without having network access. FortiToken Mobile is available for iOS and Android devices from their respective Application stores. No cellular network is required for activation.

The latest FortiToken Mobile documentation is available from the FortiToken page of the Fortinet Technical Documentation website.

Two free trial tokens are included with every registered FortiGate unit. Additional tokens can be purchased from your reseller or from Fortinet.

To assign a token to an administrator go to **System > Administrators** and either add a new or select an existing administrator to assign the token to. Configure the administrator as required, you need to enter your email address and phone number in order to receive the activation code for the FortiToken mobile. Select **Enable Two-factor Authentication**. Select the token to associate with the administrator. Select **OK** to assign the token to the administrator.

To configure your FortiGate unit to send email or SMS messages go to **System > Advanced > Email Service** or **System > Advanced > SMS Service**.

Change the default administrative port to a non-standard port

Administration Settings under **System > Settings** or `config system global` in the CLI, enable you to change the default port configurations for administrative connections to the FortiGate unit for added security. When connecting to the FortiGate unit when the port has changed, the port must be included. For example, if you are connecting to the FortiGate unit using HTTPS over port 8081, the URL would be `https://192.168.1.99:8081`

If you make a change to the default port number for HTTP, HTTPS, Telnet, or SSH, ensure that the port number is not used for other services.

Modify the device name

The name of the device needs to be modified in order for it to be perfectly identified. A label shall also be placed with the device name. Finally it shall be necessary to add an entry in the DNS with the name of the unit and its IP address.

Register with support services

In order to activate the services and warranty of the device, it is necessary to register the serial number of the device in the manufacturer's website. This task shall always be performed with the same account under which all units have been registered, in order to obtain centralized management.

Disable sending Malware statistics to FortiGuard

By default your FortiGate periodically sends encrypted Malware statistics to FortiGuard when Antivirus, IPS, or Application Control signatures are triggered. This data is used to improved FortiGuard services and determine which signatures are actively used. The malware statistics that are sent do not include any personal or sensitive customer data. The information is not shared with any external parties and is used in accordance with Fortinet's Privacy Policy.

To disable sending Malware statistics to FortiGuard, enter the following command:

```
config system global
   set fds-statistics disable
end
```

Maintain short login timeouts

To avoid the possibility of an administrator walking away from the management computer and leaving it exposed to unauthorized personnel, you can add an idle time-out. That is, if the web-based manager is not used for a specified amount of time, the FortiGate unit will automatically log the administrator out. To continue their work, they must log in again.

The time-out can be set as high as 480 minutes, or eight hours, although this is not recommend.

To set the idle time out, go to **System > Settings** and enter the amount of time for the **Idle Timeout**. A best practice is to keep the default of 5 min.

When logging into the console using SSH, the default time of inactivity to successfully log into the FortiGate unit is 120 seconds (2 minutes). You can configure the time to be shorter by using the CLI to change the length of time the command prompt remains idle before the FortiGate unit will log the administrator out. The range can be between 10 and 3600 seconds. To set the logout time enter the following CLI commands:

```
config system global
   set admin-ssh-grace-time <number_of_seconds>
end
```

Enable automatic clock synchronization

Maintain the clock in the device synchronized with the rest of the devices in the network. This facilitates auditing and consistency between expiry dates used in expiration of certificates and security protocols.

In Global configuration mode (`Config Global`), execute:

```
config system ntp
      config ntpserver
         edit 1
            set server "192.0.2.1"
         next
      end
   set ntpsync enable
   set syncinterval 60
```

```
end
```

Enable Password Policy

Brute force password software can launch more than just dictionary attacks. It can discover common passwords where a letter is replaced by a number. For example, if “p4ssw0rd” is used as a password, it can be cracked.

Password policies, available by going to **System > Settings > Enable Password Policy**, enable you to create a password policy that any administrator who updates their passwords, must follow. Using the available options you can define the required length of the password, what it must contain (numbers, upper and lower case, and so on) and an expiry time frame. The FortiGate unit will warn of any password that is added and does not meet the criteria.

Modify administrator account Lockout Duration and Threshold values

Account lockout policies control how and when accounts are locked out of the FortiGate unit. These policies are described and implemented as follows:

Administrator account Lockout Duration

If someone violates the lockout controls by entering an incorrect user name and/or password, account lockout duration sets the length of time the account is locked. the lockout duration can be set to a specific length of time using a value between 1 and 4294967295 seconds. The default value is 60 seconds.

When it’s required use the CLI to modify the lockout duration as follow:

```
config system global
   set admin-lockout-duration <integer>
end
```

Administrator account Lockout Threshold

The lockout threshold sets the number of invalid logon attempts that are allowed before an account is locked out. You may set a value that balances the need to prevent account cracking against the needs of an administrator who may have difficulty accessing their account.

Its normal for an administrator to sometimes take a few attempts to logon with the right password.

The lockout threshold can be set to any value from 1 to 10. The Default value is 3, which is normally a good setting. However, to improve security you could reduce it to 1 or 2 as long as administrators know to take extra care when entering their passwords.

Use the following CLI command to modify the lockout threshold:

```
config system global
   set admin-lockout-threshold <integer>
end
```

Keep in mind that the higher the lockout value, the higher the risk that someone may be able to break into the FortiGate unit.

Disable auto installation via USB

An attacker with a physical access to the device could load a new configuration or firmware on the FortiGate using the USB port, reinitializing the device through a power cut. To avoid this, execute the following CLI commands:

```
config system auto-install
   set auto-install-config disable
   set auto-install-image disable
end
```

Configure auditing and logging

Audit web facing administration interfaces. By default, FortiGate logs all deny actions. You can check these actions by going to **Log & Report > System Events**. This default behavior should not be changed. Also secure log files in a central location such as FortiCloud and configure alert email which provides an efficient and direct method of notifying an administrator of events. You can configure log settings by going to **Log & Report > Log Settings**.

An auditing schedule should be established to routinely inspect logs for signs of intrusion and probing.

FORTINET®

High Performance Network Security